**Task: Create IAM User with CLI Access and Enable MFA**

**Name:** Abhishek Hengade

**Batch:** B-56

This guide details the process of creating a new IAM user who can only interact with AWS via the Command Line Interface (CLI) and then securing that user's account with Multi-Factor Authentication (MFA).

**1. Understanding the Process**

This workflow involves two primary stages:

1. **Creating a CLI-Only User:** We will create an IAM user and provide them with **programmatic access credentials** (an Access Key ID and a Secret Access Key) but no password to log into the AWS Management Console.
2. **Enabling MFA:** We will then associate a virtual MFA device with the user's account. This adds a crucial layer of security, as even programmatic requests can be configured to require a temporary MFA token.

**2. Step-by-Step Guide**

**Part 1: Create an IAM User with CLI-Only Access**

**Step 1: Navigate to IAM and Begin User Creation** In the AWS Console, go to the **IAM** service. Click on **Users** in the side menu, and then click the **Create user** button.

**Step 2: Specify User Details and Access Type**

* Enter a **User name**.
* In the "Select AWS credential type" section, check **only** the box for **Access key - Programmatic access**. Do **not** check the box for console access. This is the key step to making the user CLI-only.
* Click **Next: Permissions**.

**Step 3: Set User Permissions** Attach the necessary permissions policies to the user. For this example, we will attach an existing policy directly. Select **Attach existing policies directly** and choose a policy, such as AmazonS3ReadOnlyAccess. Click **Next: Tags**, then **Next: Review**.

**Step 4: Create User and Save Credentials** Review the user details and click **Create user**. On the final screen, you will see the user's **Access key ID** and **Secret access key**. This is your **only opportunity** to view and save the secret key. Click **Download .csv** to save these credentials securely.

**Part 2: Enable MFA for the New User**

**Step 5: Navigate to the User's Security Credentials** From the IAM user list, click on the name of the user you just created. Go to the **Security credentials** tab.

**Step 6: Assign an MFA Device** In the **Multi-factor authentication (MFA)** section, click **Manage**. Select **Virtual MFA device** and click **Continue**.

**Step 7: Scan QR Code and Provide Tokens** Click **Show QR code**. The user must now scan this QR code using a virtual MFA app (like Google Authenticator). After scanning, the user provides two consecutive 6-digit codes from their app. Enter these codes into the **MFA code 1** and **MFA code 2** fields.

**Step 8: Assign MFA and Note the ARN** Click **Assign MFA**. The MFA device is now associated with the user. On the "Security credentials" tab, copy the **MFA Device ARN** (e.g., arn:aws:iam::123456789012:mfa/cli-user). You will need this ARN to authenticate with the CLI.

